CLAIMS

What is claimed is:

1. A system for proactive forced renewal of content protection implementations in devices comprising:

a key generation facility to generate and allocate keys for the devices, and to generate revocation data corresponding to revoked keys, the revoked keys being revoked in response to at least one of a security compromise and on a periodic basis independent of a security compromise; and

a device manufacturer to receive the keys from the key generation facility, to embed the keys in content protection implementations for the devices, to distribute the devices, and to renew the content protection implementations in devices after the devices are distributed, the renewal occurring in response to at least one of a security compromise and on a periodic basis independent of a security compromise.

2. The system of claim 1, further comprising a content provider to receive the revocation data from the key generation facility, and to communicate the revocation data to the devices.

3. The system of claim 1, wherein the device manufacturer receives the revocation data from the key generation facility, and communicates the revocation data to the devices.

4. The system of claim 1, wherein generation of the revocation data and renewal of the content protection implementations in the devices are performed at the same frequency.

5. The system of claim 1, wherein each device processes the revocation data prior to allowing access to protected content.

6. The system of claim 1, wherein the revocation data comprises a range of key IDs for revoked keys.

7. The system of claim 1, wherein the revocation data comprises a block of data encrypted by selected keys in a group of keys so that only non-revoked keys in the key group can be used successfully to process the data and thereby gain access to the content.

8. The system of claim 1, wherein the devices comprise consumer electronics devices for accessing protected content.

9. The system of claim 1, wherein the device manufacturer renews the content protection implementations in the devices prior to the distribution of corresponding revocation data by a selected amount of time.

10. The system of claim 3 wherein the device manufacturer communicates the revocation data to newly manufactured devices and to previously distributed devices.

11. The system of claim 1, wherein the key generation facility sends the revocation data to a storage media manufacturer for communication of the revocation data onto at least one of blank media and pre-recorded media, the media being readable by the devices.

12. The system of claim 1, wherein the key generation facility sends the revocation data to a broadcaster for communication of the revocation data into broadcast content for reception by the devices.

13. The system of claim 1, wherein the devices comprise software-implemented player applications for accessing protected content.

14. A method comprising:

receiving keys from a key generation facility;

embedding the keys in a content protection implementation for a plurality of devices;

distributing the devices; and

renewing the content protection implementations in the devices after the devices are distributed, the renewal occurring in response to at least one of a security compromise and on a periodic basis independent of a security compromise.

15. The method of claim 14, further comprising periodically receiving revocation data from the key generation facility; and

communicating the revocation data to newly manufactured devices.

16. The method of claim 15, wherein periodically receiving the revocation data and renewing the content protection implementations in the devices are performed at the same frequency.

17. The method of claim 15, wherein the revocation data comprises a range of key IDs for revoked keys.

18. The method of claim 15, wherein renewing the content protection implementations in the devices occurs prior to communicating the revocation data to previously distributed devices by a selected amount of time.

19. The method of claim 14, wherein the devices comprise software-implemented player applications for accessing protected content.

20. The method of claim 15, wherein each device processes the revocation data prior to allowing access to protected content.

21. An article comprising: a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for receiving keys from a key generation facility, embedding the keys in content protection implementations for a plurality of devices, distributing the devices, and renewing the content protection implementations in the devices after the devices are distributed, the renewal occurring in response to at least one of a security compromise and on a periodic basis independent of a security compromise.

22. The article of claim 21, further comprising instructions for periodically receiving revocation data from the key generation facility, and communicating the revocation data to newly manufactured devices.

23. The article of claim 22, wherein instructions for periodically receiving the revocation data and periodically renewing the content protection implementations in the devices are performed at the same frequency.

24. The article of claim 22, wherein the revocation data comprises a range of key IDs for revoked keys.

25. The article of claim 22, wherein renewing the content protection implementations in the devices occurs prior to communicating the revocation data into previously distributed devices.